DEVELOPMENT OF BROWSER-BASED APPLICATIONS

I. PURPOSE

This Directive provides guidance for the development -* and enhancements *- of AMS browser-based applications that will be hosted on the AMS Internet or Intranet servers. Browser-based applications are those that use an Internet browser program such as the Microsoft Internet Explorer or Netscape Navigator to run the application on the client computer. Any AMS program developing a browser-based application should reference this Directive when writing the Statement of Work or during the Requirements Analysis Phase. It should also be referenced prior to the application's development for a complete listing of application requirements.

II. REPLACEMENT HIGHLIGHTS

This Directive replaces AMS Directive 3130.3, -* Browser-Based Application Development, dated 6/9/03. *- Changes are marked with asterisks.

III. POLICY

It is the policy of AMS that all browser-based applications comply with Agency -* and Department *- standards to allow applications to be operable and efficiently administered by the Information Technology Group (ITG) and the programs. Exceptions to the use of these standards shall be approved in advance by the Chief Information Officer (CIO).

IV. AGENCY PLATFORM

Each application shall be designed to operate in the following environments:

A. **-*** Agency Internet and Intranet Servers Platform:

1. Windows 2003 (Clustered Environment);
2. Internet Information Server 6.0;
3. .NET Framework; and
4. activePDF Server, WebGrabber, and Toolkit.

The use of activePDF Server, WebGrabber, and Toolkit is not required. These are currently available on the AMS Internet servers and they have the following functions:

a. activePDF Server: Automate the PDF generation process from enterprise and web applications;

b. activePDF WebGrabber: Dynamically convert any URL, HTML stream, or HTML file to PDF while retaining styles; and

c. activePDF Toolkit: Append, stamp, stitch, merge, paint, form-fill, or secure a PDF file. *-

B. Browser-Based Applications are required to use the following environment:

1. Visual Basic.NET;
2. SQL Server 2000 -* Clustered Environment *-; and
3. Microsoft Installer (MSI) for the application installation.

Note: E-Business will provide a script for use with the MSI creation.

Exceptions to use development environments other than Visual Basic.NET for new browser-based systems must be approved in writing by the CIO in advance of any application development.

C. Client Platform:

-* Intranet-based applications shall support at a minimum the Internet Explorer 6.0 browser or higher. Internet-based applications shall support at minimum the following browsers:

1. Internet Explorer Version 5.x+
2. Netscape Version 6.x and 7.x+
3. Netscape Version 4.7x - Must provide as much functionality as possible, with the consideration that minor look and feel differences may occur compared to the latest browser versions.
4. Safari Version 1.0 (Macintosh)
5. Mozilla – Firefox ***-**

V. DEVELOPMENT PLANNING SESSIONS

A. Planning Sessions Consultation: When preparing to implement a browser-based application, the requirements must be identified to verify that the application will operate properly within the AMS environment. It is recommended that AMS programs consult with the ITG to discuss the application's requirements as follows:

1. During the development of user requirements;
2. Prior to the start of the project;
3. During status meetings;
4. Prior to application development (mandatory, see Section V.B., below);
5. During application development;
6. During the on-site installation and testing; and

7. After deployment, to ensure optimal performance.

Larger applications will require more consultation than smaller applications.

B. Mandatory Development Requirements: The following information must be provided to the E-Business Branch prior to the application development,-*of both in-house and outsourced applications *-:

1. -* Capital Planning and Investment Control (CPIC): The program shall ensure that all Information Technology (IT) investments are cost effective, well planned and effectively implemented, in compliance with AMS Directive 3130.1. *-

2. Security:

a. The security of the Agency Internet and Intranet servers is critical, -* and the risk associated with any new applications must be evaluated for any impacts to the local host and the network infrastructure. Certification and Accreditation (C&A) requirements and approvals must be accomplished prior to any application becoming operational. *- Six weeks prior to the application's deployment, the requesting program shall develop or update a System Security Plan -* (primary C&A document) *- for the application to be hosted on a server. Please contact the Agency Information Systems Security Program Manager at 202.720.1108 for assistance in preparing a Security Plan -* and any other required C&A documentation *- for the application.

b. -* The requesting program shall *- outline the development strategy to ensure conformance to the Security Plan. Be sure to address the items noted in Section VII.D., below.

c. -* The requesting program shall document how critical the system is. The documentation shall include whether the website needs to be operational 24 hours a day by 7 days a week (24 x 7) or only during working hours. If it must be operational 24 x 7, then the documentation must also include when maintenance will be performed and by whom. *-

3. Section 508 of the Rehabilitation Act:

The program shall ensure that all technology delivered complies with standards set forth in Section 508 of the Rehabilitation Act of 1973, as amended, particularly 36 CFR 1194.21-22. Outline the development strategy to ensure Section 508 compliance. For more information, see http://www.section508.gov and AMS Directive No. 3130.2, Section 508 Information Access Requirements.

4. -* e-Authentication Requirements:

Web-based applications that require user authentication (the identity of the user must be known) and/or user authorization (the identity of the user is used to determine what parts of the application the user should be allowed to access) must use the USDA e-Authentication service or obtain a waiver from the Department. This service will allow public users and USDA employees to use a single account and password to access all USDA applications that they use to conduct business. A representative of the Departmental eGovernment team can be made available at the project kick-off meeting to evaluate the e-Authentication requirements and discuss the e-Authentication implementation, if required. This applies for both in-house and outsourced applications.

Detailed information on e-Authentication can be located on the AGNIS portal site, http://agnis/sites/it/ebusiness/eauthentication/default.aspx.

5. Web Presence:

AMS is currently in the process of migrating from the current look and feel of the AMS website to the Web Presence guidelines set by the Department for Agency websites. By the end of calendar year 2005, all new and enhanced Internet applications must conform to the USDA Style Guide. All pre-existing applications will not need to comply with the USDA Style Guide until the time that they are enhanced.

The guidelines that must be followed for applications are as follows:

a. All applications must include the AMS Masthead. The AMS Masthead can be obtained from the Public Affairs office.

b. If the application requires a top navigation bar, then the top navigation bar may be customized for the application, but must include the following selections: Home, Help, and Contact Us.

c. If the application requires a left navigation bar, then the left navigation bar must resemble the AMS left navigation bar, but the selection items may be customized for the application.

The Footer consists of HTML links on two lines. The required links on the first line include: *"Application" Home* and *USDA.gov*. The remainder of the first line is reserved for application or agency specific links. An option could be *"Agency" Home*. The second line must include the following links: *Accessibility Statement, Privacy Policy,* and *Non-Discrimination Statement.*

For current guidelines or clarification, please contact the AMS Public Affairs Staff at 202.720.8998. *-

6. Bandwidth Utilization and Storage Requirements:

The requesting program shall:

a. Outline the requirements for each network transaction that uses the AMS website or Intranet site.
b. Identify the estimated number of concurrent users.
c. Identify the estimated number of total users, such as weekly, monthly, or seasonal patterns.
d. Identify the estimated size of the database (number of tables, rows per table, etc.)
e. Identify the estimated size of the application files.

7. Hosting Strategy:

The requesting program shall:

a. Identify if the application will be Internet or Intranet based.
b. Identify if the Agency or program will host the application, if it is Intranet based.

Note: All Internet applications shall be hosted on Agency-owned servers operated by ITG. Intranet applications may be hosted either on the Agency Intranet server or on a program-owned Intranet server. All Internet and Intranet servers shall comply with Agency and Departmental security standards and will be subject to periodic security audits. ITG shall be responsible for securing and maintaining Agency-owned servers. The programs shall be responsible for securing and maintaining program-owned servers. If applications are hosted on Agency-owned servers, each program is responsible for maintaining the unique functionality of their application and ITG is responsible for server functionality.

8. Application Maintenance:

a. Describe the backup strategy for the application (e.g., How often must backups be completed? Who will be performing the backups?).

Note: Applications hosted on Agency-owned servers shall be backed up by ITG. Applications hosted on program-owned servers shall be backed-up by the program. Specific backup documentation is described in Section VII.C.

b. Describe the warranty or maintenance requirements of the system (e.g., Will the vendor correct any problems for 6 months following deployment?).

c. Describe how the unique functionality of the application will be supported by the program or a contractor (e.g., if the application contains an error, how will the program or a contractor resolve the issue?).

VI. RESPONSIBILITIES

A. The AMS Program developing the application shall work cooperatively with ITG and the E-Business Branch throughout the lifecycle of the project as described in Section V., above. -* For each application, form ST-19, Browser-Based Application Development Agreement, must be completed and submitted to E-Business prior to application development. This applies for both in-house and outsourced applications. *-

B. ITG and the E-Business Branch shall:

1. Provide pre-project consulting regarding the AMS environment;
2. Provide technical consulting and support during the development, implementation, and deployment phases of the project; and
3. Provide infrastructure support during the lifecycle of the application.

Neither the contractor nor the program shall discuss Internet application features or availability with the press prior to clearing this communication with the Public Affairs Staff and obtaining the concurrence of the E-Business Branch.

VII. DOCUMENTATION

Each browser-based application must have user, system, backup, and security documentation prior to implementation, as described below. -* Each application must be certified and accredited by the appropriate Agency official in advance of its deployment as a production system. The Letter of Accreditation and other system and backup documentation is to be submitted and reviewed by ITG prior to application deployment. Security documentation must be provided to ITG six weeks prior to the application's deployment. *-

A. User Documentation: User documentation shall be provided to instruct the users in all facets of the application's functionality. The user documentation must be in the form of on-line help, and the following items are recommended:

1. Purpose of the application;
2. Step-by-step instructions on how to use the application, including screen captures;
3. A glossary of terms; and
4. Help or trouble-shooting guidance for each data field.

B. System Documentation: System documentation shall be provided to ITG prior to implementation for full support of the application. -* Application installation instructions must be provided to ITG prior to installation onto the test application server. *- The system documentation must include a minimum of the following items:

1. Purpose of the application;
2. A listing of the hardware and software system requirements;
3. Detailed tables and structures (i.e., field definitions, views, table relationships, and stored procedures);
4. A listing of each file in the application, its location, and a description of its use;
5. A listing of the dependencies, such as, required permissions, DLL files, DSNs, supporting software/hardware, etc.;
6. A listing and description of any custom components that have been developed (i.e., Active X components and custom DLLs);
7. A listing of any application created files and their formats;
8. A listing of the stress and other testing that has been performed and the results;
9. A listing of likely failures and how to troubleshoot them;
10. A detailed set of installation instructions; and,
11. A program contact person to assist in support and troubleshooting.

C. Backup and Recovery Documentation: Data on the Internet is subject to the possibility of unauthorized access. For every application, a reliable backup source needs to be available in the event of data corruption. -* Backup and recovery documentation must be submitted to and reviewed by ITG prior to the deployment of the application. *- The backup and recovery documentation must include, at a minimum, the following items:

1. A listing of the files to be backed up;
2. A description of where the files are backed up;
3. A procedure documenting how the backup is performed and with what utility;
4. Who performs the backup;

5. A description of the procedure required to determine if the data has been compromised;
6. A description of how often this procedure is run and who performs it;
7. A listing of files that must be restored in the event of data corruption;
8. A procedure documenting how a restore is performed and with what utility;
9. Who performs the restore; and,
10. A program contact person to assist in support and troubleshooting.

D. Security Documentation: Security documentation is critical for maintaining the integrity of the application and must be provided to ITG six weeks prior to the application's deployment. The security documentation -* typically shall be the System Security Plan that includes responses to the following questions and information: *-

1. Who will be using the application? Will it be used exclusively by the Agency or by the public as well?
2. How will the application be accessed -* and who will access the application? *-
3. Who will be performing administration of the application?
4. -* Are there any special ports or Firewall requirements? *-
5. Provide a listing of general user permissions required for using the application.
6. Provide a listing of administrative permissions required for application maintenance.
7. Is the entire application available to the general user or are certain areas restricted?
8. What security method is used to restrict access to the entire application?
9. Does the software require that any additional service packs or hot fixes be applied to the supporting software? If so, list the required service packs or hot fixes. If hot fixes are required, will they need to be reapplied after system changes?

E. -* IT Continuity of Support Plan: An IT continuity of support plan describes how to sustain major applications and general support systems in the event of a significant disruption. This plan will include the disaster recovery plan, for continuing critical operations during a significant disruption, and the business resumption plan, for returning to normal operations following the disruption. An IT continuity plan must be developed for each major application and general support system.

1. Disaster Recovery Plan: A disaster recovery plan applies to major, usually catastrophic, events that deny access to the normal facility for an extended time period. Frequently, disaster recovery plans refer to a plan designed to the operation of the targeted system or application at an alternate site after the emergency. The disaster recovery plan scope may overlap that of the business resumption plan; however, the disaster recovery plan is narrower in scope and does not address minor disruptions that do not require relocation.

In 2005, to implement AMS' website disaster recovery plan, AMS will be implementing an off-site location for continuing Internet operations in the event of an extended downtime at headquarters. This off-site location will be housed in Denver, CO, and will include the AMS Website, associated critical applications, and the Market News wire information. Each application housed on the AMS web servers must have an associated plan to incorporate into the Continuity of Operations Plan (COOP).

If the application is determined to be mission critical, it must include the following items:

a. Identify activities, resources, and procedures needed to sustain operations during prolonged interruptions. These procedures will include detailed instructions for switching to the off-site location and then switching back to headquarters.

b. If the application has a dynamic database, then detailed instructions for updating the database at headquarters must be included. This process should be automated, such as the running of a script or batch file.

c. Include a listing of possible problems during the switchover and their resolution.

d. Assign responsibilities to designated personnel and provide guidance for recovering the application during prolonged periods of disruption.

If the application is determined not to be mission critical, an acceptable amount of downtime must be identified and the plan must include alternative methods for the application's functionality.

2. Business Resumption: A business resumption plan is a set of instructions or procedures that describe how operations will be restored after a significant disruption has occurred. This plan will include the criticality of the application and the amount of acceptable downtime.

F. Configuration Management Plan: All personnel responsible for making changes on the system, such as an application upgrade, must document the items below, ensure appropriate segregation of duties in the change process, and receive all appropriate management and program technical approvals for the proposed changes, prior to implementing the change.

1. Who is the requestor of the change?
2. What is the change?
3. What is the reason for the change?
4. What is the impact on customers during implementation?
5. What is the date and time the change is scheduled?
6. Is there a system outage required? If so, what is the duration of the outage?
7. Will users be notified in advance of the proposed change? If so, how and when will they be notified?
8. What are the risks associated with the change? What problems or symptoms are likely if the implementation is not successful?
9. Who will test the change? How will it be tested?
10. Who will review the test results?
11. What are the procedures for implementing the change?
12. What are the back-out procedures for the change?
13. What is the impact on customers if the implementation is successful?
14. What is the impact on customers if a back-out is necessary?

G. Records: The e-business process is not properly documented until a record of each business transaction has been identified and properly protected. The following guidelines and procedures will assist employees in determining the proper procedures for protecting Federal records.

1. Creating Records: The employee creating the information, or receiving information from outside of AMS, is the person responsible for maintaining the record copy. All other copies are for informational purposes only, and may be destroyed when no longer needed, in accordance with National Archive and Records Administration (NARA) guidelines.

2. Disposition Instructions: The authorized disposition instructions for AMS records are contained in the General Records Schedules and the AMS Unique Records Schedules. All records accumulating in AMS, regardless of the form, will be maintained and disposed of in accordance with these schedules. Any deviation of these procedures is a violation of the Federal Records Act (FRA).

For assistance contact the AMS Records Management Officer at 202.720.0566. *-

VIII. OUTSOURCING

When an application is constructed and implemented using outside contractors for deployment on the AMS Internet or Intranet, the following requirements shall be addressed within the Statement of Work:

A. The contractor shall meet with ITG and program personnel prior to application development to discuss the AMS Internet/Intranet environment and any special requirements that the application may need. At this time, ITG must be provided with bandwidth, server, and other IT related requirements.

B. -* The contractor will be required to meet all specified Security requirements depending on the application and where it will be hosted (e.g., Personnel physical access, Identification (badges)/escorts, background checks or clearances as required), *-

C. The contractor shall do all development and testing using non-infrastructure equipment. The AMS infrastructure equipment will not be made available for these activities.

D. The application shall be shown to work according to contract specifications prior to deployment on AMS infrastructure equipment.

E. Initial deployment will occur on the AMS developmental server during non-business hours (e.g., Sunday or early morning on a weekday with installation, testing, and rollback, if necessary, completed by 7 a.m.).

F. The contractor shall install the application -* on-site, *- on AMS infrastructure equipment under ITG supervision, along with program personnel.

G. ITG must be given a minimum of three days notice when scheduling a contractor to install the application or any updates.

H. Actual deployment will occur once the application has been shown to work within the AMS Internet/Intranet environment, according to contract specifications.

I. The contractor will hold a post-deployment, knowledge-transfer meeting with ITG and program personnel to discuss system maintenance and provide detailed system documentation.

J. Copies of the application software will be provided to ITG with detailed installation procedures.

IX. QUESTIONS

If you have any questions concerning browser-based application development, contact the E-Business Branch, Information Technology Group.

/s/

Lloyd C. Day
Administrator

Attachment